Argentina: The Challenge Of Information Operations

By Dr. Javier Ulises Ortiz

Dr. Ortiz discusses several policies and strategies for protecting Argentinean and coalition critical infrastructure. He describes the functions of the Armed Forces Scientific and Technical Research Infrastructure Institute, a joint military organization that possesses an information security laboratory. He further explores the Argentine Defense Forces' creation of "computer science troops" in its Communications and Computing Systems Command.

Introduction

Ten years have passed since US military systems were cybernetically-electronically attacked by means of a computer network from an unknown country—an event known as "Solar Dawn." The 9/11 attacks and other events, like the massive blackouts in big urban settings, demonstrate that unlimited security in a complex world is impossible.

Cyberspace is the new "Athena´s Camp" in today's conflicts, especially "asymmetrical" ones. In developed countries the concepts of information warfare (IW) and information operations (IO) have appeared as new military doctrines.

According to sociologist Manuel Castells, 9/11 was the beginning of the first world war of the 21st century, the "net war" initiated by weak forces attempting to "impose their objectives by using the only efficient weapon in its technological and military inferiority situation." In May 2007, the Estonian computing system was attacked by half a million computers, via the Internet. Estonia was paralyzed for weeks and needed NATO's help to recover. NATO spokesman James Appathurai noted "the XXI century is not one of tanks and artillery." He further summarized a June 2007 NATO chiefs meeting saying "everybody agreed that it is indispensable to improve the protection capability of the computing systems of critical importance."

As an answer to these attacks, a new concept in defense and security matters appeared: the Protection of Critical Information Infrastructure (PCII). It is necessary to identify and secure the CII to avoid new "Mutual Assured Destruction" vulnerabilities in this new age. Cooperative agendas for regional and defense security issues must incorporate CII-related definitions, so that member countries develop their own concepts. Telecommunications (optical fiber, digitalization, computing) represent the technological infrastructure of globalization, making strategic decision-making in real time possible on a global scale.

Argentine national flag. (Wikimedia)

Nations can take on elements of new forms like the "Digital State" or "Net-State," and a nation's sovereign territory then undergoes change in leaders' minds. Whether by attack or by accident (such as a blackout in a megalopolis), the risks associated with not having preventative systems, early warning, and fast answers based on emergency plans, can be devastating.

The main objective of these new types of conflict is the destruction or disability of information capabilities and critical infrastructures. This understanding of war as "not only military" has been developed in different parts of the world. Different documents in the USA, Europe, and other countries start to define the issue and to generate doctrine for action. Information space and "physical" critical infrastructures are strategically linked. Thus, network warfare is more about organizational doctrine than technology.

The following US definitions are used in this article:

• Critical Infrastructure: systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

• Information Operations (IO): Joint Doctrine's first IO definition in 1998 was changed in 2003 (the definition of Information Warfare was removed completely, leaving only the definition of Information Operations). The February 2006 doctrine says IO shall: "… integrate the employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operation security (OPSEC) in concert with specified supporting and related capabilities to influence, disrupt, corrupt, and usurp adversarial human and automated decision-making while protecting our own." IO doctrine is in constant evolution, as shown by the February 2007 US Army update which "uses the joint definition of IO as well as all capabilities that compose IO; however, Army doctrine categorizes IO capabilities in themes of five IO tasks: information engagement, C2 warfare, MILDEC, OPSEC, information protection."

Latin America had its first important computer security-related challenge in 1999, when facing the Y2K problem. Recently, new definitions related to military information technologies started to appear in many Latin American countries. Many nations are updating definitions and doctrines. This article includes: strategic perspectives for analyzing IO issues; the development of hemispheric strategies for the PCII and cyber security; Argentinean recommendations for countering extremist views on the Internet; the Argentine military doctrine related to IO; the Argentine military and other Latin American countries understanding of IO; and conclusions.

A Strategic View for Analyzing the Issue

In a changing world, conflicts become highly complex. Our concept of conflict, defined along a line from declared wars to undeclared wars, becomes more diffuse between these limits. Presently, we see continuous changes in regional military strategies, doctrines, capabilities, organizations, land operations, and procedures. Hence, it is more efficient to analyze Argentina's doctrine by including elements of NATO's IO doctrine. Yet, even NATO still does not define cyber attacks as military attacks. These wars of probable "zero casualties" can be analyzed from different perspectives, all of which include the impact of information technologies—and the potential devastating consequences. It is important to analyze different doctrinal models based on "real," and not "potential" capabilities.

Hence, it is necessary to analyze laws, policies, and national and regional strategies. Only then can one understand that information age conflicts are global, that military forces and doctrine are part of a nation's public sector, and that together with the private sector they constitute the critical and information infrastructure facing the cyberspace threat. We must consider all these elements, but even more explicitly in countries where the technological gap is wider, and the infrastructure is more vulnerable.

Hemispheric Strategies for Protection of Critical Information Infrastructures & CyberSecurity

During the last five years, Organization of American States (OAS) member countries signed agreements forming the basis for PCII and cyber security, as follows:

1. Civil and civil-military cooperation in the fields of Defense and Security is necessary, according to the five Ministers of Defense of the Americas Conference (Santiago de Chile, November 2002). They noted "The Hemisphere faces an increasingly diverse and complex set of threats and challenges for its states, societies, and people," and that "each American state is free to choose its own defense instruments including the mission, personnel, and the composition of Defense and Security Forces needed to guarantee sovereignty, in accordance with UN and OAS Charters." There is also a "particular strategic context of each sub-region in the Hemisphere."

2. The Defense "White Book:" (Officially the *Adoption of the Guidelines on Developing National Defense Policy and Doctrine Book.)* This is a key policy document providing the government's vision for defense of the OAS (2002).

3. The OAS's "Declaration on Security in the Americas" (October 28, 2003: This agreement notes the new concept of security in the Hemisphere is multidimensional in scope, and includes traditional and new threats, concerns, plus other challenges to member states, incorporating the priorities of each state. Traditional threats, new threats, national concerns, and other diverse challenges affect member states in different ways. New threats include attacks on cyber security, and "new terrorist threats—whatever their origin or motivation—such as threats to cyber security, biological terrorism, and critical infrastructure.

4. An Inter-American strategy to combat threats to cyber security: Together with Argentina, Canada, and Chile, the US OAS delegation presented this document May 19, 2003. This important strategy is key to the development and consideration of a common vision of critical infrastructures for all the Americas. The document notes "A multidimensional and multidisciplinary approach to create a culture of cyber security" must be developed in order to protect the infrastructure of telecommunications. It gives responsibilities to:

- The Inter-American Committee against Terrorism (CICTE): The formation of an Inter-American Alert, Watch, and Warning Network is needed to rapidly disseminate cyber security information and respond to crises. Creation of a Hemispheric network to support Computer Security Incident Response Teams (CSIRTs) is also required.
- The Inter-American Telecommunications Commission (CITEL) was formed to identify and adopt secure Internet architecture technical standards, in 2004.

5. Protect Critical Information Infrastructures (PCII): International cooperation is the key to protection of essential information infrastructure, coordination of early alert systems, analysis of vulnerability, threats, and incidents—with regard to information and to coordinate investigations of attacks against said infrastructures according to national legislation. This information can be found in the *Blue Book: Telecommunications Policies for the Americas* (2005).

6. Hemispheric Definition of Critical Infrastructure (CI): This "refers, among others, to those facilities, systems, and networks, and physical or virtual IT services and equipment, the disabling or destruction of which would have a severe impact on populations, public health, security, economic activity, the environment, democratic governance, or the ability of the government of a member state to operate effectively." This important document is key to consideration of a CI common vision in the Americas. OAS, (March 1, 2007).

Argentina's Recommendations for Countering Extremist Views on the Internet

Argentina created a national system to face these challenges:

1. The Information Technologies National Office (ONTI) is part of the Ministries Office Chief. ONTI is responsible for creating technological development and innovation policies, in order to transform and modernize the state. On August 3, 2005, ONTI approved the "National Public Sector Information Security Policy" for the development of Information Security Policies in each public area (regulation ISO/CEI 17799).

2. Argentina's Computer Emergency Response Team (ArCERT). ArCERT started operations in May 1999 under ONTI. Main roles are:

- Centralize security incident reports that take place in the Federal Administration, and facilitate information exchanges in response.
- Provide a specialized advisory service for network security.
- Enhance the coordination among federal organizations to anticipate, detect, handle, and recover information from security incidents.
- Act as a repository of information for security incidents, tools, and defense technologies.

ONTI and ArCERT define the following concepts:

- Information: every communication or representation of data or knowledge, in any form (text, numeric, graphic, cartographic, orthographic, or audiovisual) and by any media (magnetic, paper, PC, audiovisual, or other).
- Information systems: independent sets of information resources organized to summarize information's processing, maintenance, transmission, and distribution by different processes (manual or automatic).
- Security Incident: a negative event in a PC system, or PC net, that compromises the confidentiality, integrity, and availability of information. It can be caused through vulnerabilities or attempts/threats of breaking into an information security infrastructure.
- Threats to Information Security: actions against the confidentiality, integrity, and availability of information. These threats can be caused by human error, attacks, or catastrophic accidents.

3. The Homeland Security System has the following additional offices with responsibilities for the security of the information infrastructure.

- The Federal Police Division for Technological Crimes cooperates with Justice's investigations on criminal issues.
- In the National Defense System, the Armed Forces Scientific and Technical Research Infrastructure Institute (CITEFA) is the only joint military organization dedicated to scientific and technological activities allowed to conduct research and development to meet Argentina's National Defense requirements.
- The Information Security Research & Development (SI6) Office is CITEFA's Lab. It was officially created in January 2004 to develop information security R&D activities for both general and defense areas. SI6 belongs to the Information Security Division of the IT Department. Actually, SI6 is working on intruder detection, intruder classification, intruder identification, honeypots, pattern analysis, biometric authentication, virtual private networks, firewalls, digital signatures, penetration tests, and other issues. SI6's mission is the generation of information security knowledge through research & development activities. The SI6 Lab considers the sum of community efforts in applied research, using innovative technologies as one of the most efficient ways to build technological knowledge. SI6's working projects include: "Paranoid: Intruder Identification System using Honeypot Techniques;" "BioVpn: An Open-source Biometric Authentication Process for VPN;" and "Cisilia: A Windows NT/2000/XP Password Cracking Distributed Application for Linux Platforms Using Open Mosix Clusters."

Argentina's Military Doctrine Related to IO

Before analyzing the definition of IO it is necessary to look at background information on Argentina's Structure for National Defense:

Argentine provinces. (Wikimedia)

1. The National Defense System. Law N° 23.554 de 1988 defines National Defense as the integration and coordination of all forces of the Nation for the solution of conflicts that require the use of the Armed Forces, in a dissuasive or effective way to counter external aggression. Its scope is to permanently guarantee the sovereignty and independence of Argentina, to protect its territorial integrity and self determination, and to protect the life and freedom of its inhabitants.

The Armed Forces primary responsibility is to defend the country against military aggression from other states and protect the nation's sovereignty and territorial integrity. Homeland Security Law N° 24.059 establishes that police and security forces must be used in case of criminal actions, while the Armed Forces can, only in special cases upon request from Homeland Security Officials, confront threats of a non-military nature.

In 1998, the Defense Ministry published the *White Book for National Defense* in which it analyzed "the

Revolution of Military Affairs" (RMA). The RMA changed the quantitative criteria for "soft power." This concept has three axes: space military information, soft power's use in processing elements (in systems C3I2), and soft power's use in precision weaponry. The White Book also underscores a new danger: the threat to Argentina's own computer systems. A 2001 update to this book includes a strategic view of the RMA (with IT) and how this changed the "art of war." This required changes in military doctrines, in weapon systems, and in the logistical and organizational structures. This document further established the need to integrate C4I2 and electronic warfare systems at the national, military, and operational-strategic levels; and included the satellite systems applicable to Defense.

Decree N° 727/06 strengthened the role of the Joint Military Staff (EMCO) as the main military strategic decision-maker under the civil government.

The mission of Chief VI - C3I2 - EMCO (Command, Control, Communications, Intelligence, and Interoperability) is to develop and control the policies, plans, programs, and projects of the C3I2 joint and combined staffs, and to provide a Joint Military Doctrine for Communications and Electronic Warfare. Each of the Argentine armed forces has similar areas. The Argentine Army has the Communications and Computing Systems Command, staffed by specially trained personnel, to include "Computer Science Troops" and officers with advanced Computer Science degrees.

2. Military doctrine related to IO. In Argentina, military doctrine is the systematic organization of principles, definitions, regulations, and procedures that constitute military knowledge—and offer satisfactory answers to military problems. Doctrine is the basic and active element in force design, including Joint Military Doctrine, Naval Military Doctrine, Air Force Military Doctrine, and Army Military Doctrine. These regulate the services' actions to fulfill their missions as military components, and fundamental institutions of the nation. In 2007, Argentina adopted a Defensive Strategic Operational Attitude by means of a deterrence policy derived from the Argentine Army Chief of the General Staff's "Argentine Army 2025" vision. This plan takes into account the peace and cooperation zone created by the Southern Common Market (MERCOSUR), including the Regional Trade Agreement (RTA).

The *Regulation for the Conduct of the Land Military Component* establishes that secure communications are the essence of C2 so that the commander can influence operations effectively. Many IO elements are incorporated in Argentina's military doctrine. As many Argentine military authors note, the diverse elements that constitute IO are defined by Argentina's army military doctrine. The *Dictionary of the Argentine Army* defines operations linked with IO as follows:

Military Operations: military activities for situations when facing a real enemy. This includes employment and direction of dependent elements, to execute mission needs;

Electronic Operations: complementary operations conducted through the use of communications and special communications electronic media, in order to support other operations throughout the electromagnetic spectrum for their benefit while restricting or avoiding its use by the enemy;

Special Operations: operations different from others, either because they have particular procedures, organizations, or media, or because there is a need for specially trained forces. Special operations can be executed through conventional or non-conventional means;

Non-Conventional Operations: those executed on enemy territory or on friendly territory occupied by the enemy, and within the scope of attaining designated objectives;

Complementary Operations (military deception): multiple, synchronized actions to hide from the enemy the true intentions of one's own forces.

Peacekeeping Operations: operations to support diplomatic efforts of international organizations to maintain, restore, and/or enforce peace in a conflict zone.

Psychological Operations: those operations that use psychological actions in a planned way to influence the behavior and attitudes of selected individuals or groups, with the aim of facilitating the development of one's own operations. At the operational-strategic level these operations contribute to:

- Diminishing the morale and fighting strength of the enemy;
- Increasing one's own and one's allies fighting strength;
- Obtaining the help of neutral parties.

Civil Military operations: support special disaster situations.

C2TI. IO doctrine includes C2TI (Command, Control, Telecommunications- Computer Science, and Intelligence) as the set of human and technological resources and procedures that allow the commander and his staff to control, communicate, and know the enemy situation in real time. This abbreviation includes the other concepts of C3I and C4I.

Electronic War: a set of military activities developed in the electromagnetic spectrum, with the purpose of providing:

- Electronic Support Measures: those that determine the presence of enemy activity. These are offensive measures (search, intercept, localization, analysis, identification, and evaluation among others);
- Electronic Support Countermeasures: those that neutralize and/or reduce the use of electromagnetic energy dispersed by the enemy. These are defensive measures (such as deception and interference);
- Electronic Support Counter-counter measures: those that guarantee the electromagnetic energy dispersed by one's own means. These are offensive measures (counter-deception and counter-interference);

Army doctrine considers electronic war as an essential part of every war. Its characteristics are that it:

- Is permanent, secret, complex, and utilizes highly trained personnel;

- Is adaptable to planning, centralization, and the conduct and coordination with other electromagnetic activities;
- Is flexible and adaptable to military maneuvers but possesses security measures;
- Is used in tactical surprise and provides speedy assessments.

Computer, Electronic, Cryptographic, and Communications Security: The Functional Regulations of Computer Systems used in the Army (RFD-75-01) contain the general rules for data administration and management for the forces' computer security and define the following:

- Computer Science: is the joint technique for the automatic use of information. Computing is important for military operations;
- Telecommunications & Computer Science: is the association between telecommunications and data processors' technical effects that help process information;
- Computer Science Troops: military personnel who maintain an efficient security system that avoids both the loss of information and non authorized access to the data;
- Kinds of Computer Security: Electronic Security, Communications Security, Cryptographic Security, Transmission Security, Computer Systems Security, and Physical Security.

Education related to IO. In different educational institutes of the Education and Doctrine Command of the Argentine Army and its higher educational institutions, personnel develop the following courses including some aspect of IO:

- Technical Higher School of the Army (EST): offers Degrees in Computer Systems Engineering, a postgraduate course in "Computer Systems, Cryptography, and Security," and a "Master in Technological Management." The EST participates in the organization of the National and International Congresses of the Telecomputing and Cryptographic Systems Security shows (CONSECRI) where civilian and military experts from Argentina and the Region exchange knowledge on cryptography, cyber attacks, IO, security, and others issues;
- The Higher School of War (ESG) has a Tactical Trainer (ADITC) with simulation software that trains commanders and staff and in a General Staff Course the curricula includes some aspects of IO. For this reason many officers consider monographs or thesis related to IO in their studies;

Malvinas War Memorial in Buenos Aires (Wikipedia)

- School of Communications develops technical courses for military specialists and provides specific doctrine to employ the communications corps;
- School of Computer Science, created in 1992, has courses in Computer Security Science;
- Other Navy and Air Force institutes, and other public and private universities such as Buenos Aires Technological Institute (ITBA), also have courses on this issue;
- The Argentine and Chilean Armies jointly developed a Training System for Peace Missions (SIMUPAS), a virtual peacekeeping operation.
- AFCEA Argentina is the South American chapter of the Armed Forces Communications and Electronics Association (AFCEA International) that unites specialists in C4ISR. AFCEA develops military and civilian courses in IW, IO, cyber attacks, and PCII.

Argentine Military Understanding of IO

The Malvinas War (1982) [*editor's note: also called the Falklands War*] served as the baptism by fire of the Communications Units of the Argentine Army, in conventional operations. This war marks the first reference to the "Computing Revolution" as applied to telecommunications, and especially to electronic warfare. In 1999, the Argentine Army first evaluated the impact of information technologies, by examining the use of the Internet and satellite connections between other elements. As a result, Argentina created a unified Army Communication and Computing System Unit, with a digital net for the Systems Integration of the Army (REDISE).

Argentina's evolving military understanding of IO over the past five years is as follows:

- Argentina has an IW doctrine - The Argentine Armed Forces have specific doctrine on cybernetic war issues to include some restricted issues. The Argentine concept of EW (electronic warfare) is valid for IW (Commander of Argentine Navy G. Repetto, 2001);
- Strategic IW - In strategic IW, it is necessary to apply "the enemy as a system" theory of Colonel John Warden, attacking the C4ISR of an enemy while maintaining capabilities in C2 & TI. The threats to the national information infrastructure are real, non-traditional, and highly diversified. It is necessary to develop operational concepts and structures to have superiority on the new

battlefield (Colonel, Ret., of Argentine Army, AA, H. Cargnelutti, 2002);

• Cybernetic Strategy - Capturing cyberspace's power requires a Cybernetic Strategy to organize the Cybernetic Force and develop new weapons. New national and international laws are necessary. Cyberspace, where "cybernetic operations" are conducted, is not limited as is the traditional battlefield. Hence, its duration and operational range is wider (Col A.A. and Veteran of Malvinas War, E. Stel, 2002).

• Basic Objectives of Military Computer Security - The security of the military computer system must accomplish four basic objectives: confidentiality, confidence, integrity, and disposability of information. IW is offensive, and it is necessary to train military personnel how to enter enemy nets. This organization would be the Army's "hackers" in conflict situations. (Captain F. Calvete, Military Engineer in Computing Systems of A.A., 2003).

• Future Wars - These will involve IW. Modern armies must protect their own information and nets, and attack the same capabilities of the enemy on the new cyberspace battlefield. (Col. A.A. Cerezo, 2003).

• Need for new Strategic Military Thought in the Information Age - Argentina's National Defense System doctrine must include IW and IO concepts. IW/IO Commission, the Center of Strategic Studies, and the School of War are all doing work in these areas (CEE-ESG, 2003).

• Definitions - Argentina does not strictly adopt the standard IO Definition, but the Argentine Armed Forces Information System is used in the IW context. Argentine cyber military doctrine is oriented toward a security perspective, with IW as an asymmetrical threat. If the Argentine Armed Forces include IW concepts in their doctrine, it can only help toward the identification of operational and I+D capabilities for asymmetric war. It will be necessary to incorporate both defensive and offensive IO within the definition of future complementary operations (for example, military deception). Even though there is not a doctrinal definition of IW in computing systems, there is increasing interest in the application of these concepts (Majors A. A.Machinandiarena and Tabeada y Gaidano, 2003).

• IO is Part of Asymmetrical War - IO includes attempts to deceive or undermine the capabilities of enemy forces. Offensive IO includes infrastructure attacks, PSYOP, and misinformation. It is only necessary to have a PC, a modem, and a program to get into an enemy's C4 or weapon system. (Major A.A. Machinandiarena, Battalion 601 of Electronic Operations, 2004).

• Strategic Operational Dislocation in New Wars - Dislocation is achieved through a direct or indirect approach against an enemy force, to cause an imbalance in their forces, disconnect elements of their command, affect their moral and maneuver capability, or to weaken their defenses. Dislocation can be achieved via technological and digital capabilities, which can be improved still further with the use of IO (Col Roberto Pritz, Director of the Higher School of War of A.A., 2005).

Latin American Countries' Understanding of IO

In the Latin American region there are other studies related to IT in military affairs. Homeland Security Departments include many IT security aspects in their respective areas of responsibility. In the military camp, there are fewer precise definitions of IO/IW. However, as is the case with Argentina, IO is part of military study groups, and many IO-related opinions have a national basis:

• Strategic Information Warfare (SIW) - This refers to the use of computer systems against the critical infrastructure (CI) of a country. It is the new way to conduct "war and anti-war" (Alvin Toffler). Brazil has created several responsible offices designed to defend the countries critical infrastructure. (Commander Riquet Filho, Brazil Navy, 2003).

• Cyber War is Not Yet Uniformly Defined - Cyber war can be understood as measures taken against C2 systems, operational security, electronic war, piracy, hackers, and information blockades. Since 2003 the Brazilian Navy has established rules of digital information management for their local nets (Commander Nascimento de Annunciacao, Brazilian Navy, 2003).

• Cyber War - This concept corresponds to the offensive and defensive use of information systems and information to deny, explore, corrupt, or destroy adversary values and information systems as well as computer networks. Cyber war attempts to obtain advantages in both the military and civilian realms. Twenty countries are preparing cyber guerillas as "elite troops" (4th Computing Systems Security Committee Meeting, Brazil Ministry of Defense, 2003).

• Cyber Terrorism Post 9/11 in the Western Hemisphere - The inability to accurately track cyber attacks may give the impression that there are a lower number of incidents in Latin America—which is wrong. History indicates political and military conflicts are increasingly accompanied by cyber attacks. A large percentage of military traffic moves over civilian telecommunications and computer systems. Trends seem to point to the possibility of terrorists using information technology as a weapon against critical infrastructure targets. Regional exercises are one of the best ways to assess such critical infrastructure vulnerabilities. There is a significant difference in the usage of computers and the Internet between Latin America, the Caribbean, and North America. International collaboration and cooperation is important to ensure security of international networks, which would in turn make local systems more secure. (Lt. Col Wanda I. Cortes, US Air Force Reserve, Inter American Defense College, 2004).

In July, 2007, the Colombian Telecommunications Committee published a study for the implementation of a National Strategy for Cyber Security. This report considers security of communication nets a secondary preoccupation for most countries in the region. Some Latin American nations have begun adopting information security labeling procedure (rule ISO/CEI 17799), but there is a juridical weakness.

- Identification of Critical Infrastructure - Mr. Arístides Royo, Ambassador of Panama to the Organization of American States (OAS) and Chair of the Inter-American Committee against Terrorism (CICTE), announced in March 2007 that CICTE will soon begin to review its work plan. It is likely the organization will identify areas related to critical infrastructure, both in physical terms (ports, etc.) and in terms of the so-called "virtual variety."

Conclusions

During the course of history, war was fought on open battlefields. During the twentieth century, with the development of the submarine and air power, war extended its horizon from one to three dimensional battle spaces. A fourth geo-strategic battle space was also created near the end of the millennium: cyberspace. At the beginning of the twenty first century, the dimensions of war are as foggy as they are clear, as Admiral William Owens explained in his *Lifting the Fog of War*. For the military commander, the contemporary battlefield is full of difficulties—the Net has produced a new fog of war. Cyber war forces changes in many of our objectives, strategies, doctrines, and procedures. In these new conflicts, C2TIs bring different capabilities to commanders. But the C2TIs bring new vulnerabilities too because all the public-private critical information infrastructures are integrated, and one effective attack could generate multidimensional "cascade effects."

Within the Organization of American States (OAS), the countries of Latin America and North America agreed to a common vision of cyberspace threats, and to the first lines of protection and reaction—both physically and virtually—against them. In Latin America this situation requires the elaboration of relevant national, bilateral, and multilateral policies and strategies. It is first necessary for all member countries to secure critical information infrastructures. Each organization, especially military forces, needs to be prepared and trained to remain mobile and to generate influence (in terms of power) on a global scale. Argentine and other Latin American armies have general doctrinal concepts to confront the new challenges in cyberspace. They can help support one anothers' responsibilities along with other public areas, to include not only their countries, but also regional protection of critical information structures.

Regional military forces should permanently update their doctrines in order to generate methods, techniques, and training. Each country should develop new doctrines according to its own capabilities and national realities, to support both bilateral and multilateral mechanisms of cooperation. Those who have updated doctrines can confront new situations with confidence. In his "Strategy for Action," the French strategist General Beauffre reminds us "it is necessary to act as a thoughtful man and to think as an action man" —because the future is now.